FIVE MUST-KNOW FACTS
ABOUT THE DIGITAL TRANSFORMATION AND COVID-19

Introduction

The transformation from analog devices to digital processing is well underway. The worldwide-installed base now numbers 1.333 billion computers.[1] In addition, there are 3.3 billion smartphone users around the world[2] as well as 7 billion IoT devices online. Adding in automotive computing and other miscellany brings the total to 17 billion connected digital devices.[3] Despite this mass of processing power, the migration to digital technologies is far from complete. The COVID-19 pandemic is forcing organizations of all kinds to accelerate the digital transformation and modify their networking and security strategies. It's happening like this.

Due to the current pandemic, among "knowledge workers" who work primarily on computers, at-home users and mobile users are now the majority. These include employees, customers, partners and investors each of whom require different types of connectivity and privileges. In addition, automation and AI are removing human workers who are susceptible to COVID-19 from work processes altogether.[4] Likewise, travel barriers and other factors are making telepresence and branch offices more prominent.

The result is completely distributed IT operations. This means mean your networking strategy for providing mission-critical services must change its arc. The cyber security you must use to protect your changing environment must follow these changes. Here are 5 facts you must take into account when adapting your networking and cyber security to the new normal brought about by today's pandemic.

[1] Statista, Installed base of personal computers (PCs) worldwide from 2013 to 2019 (in millions), as viewed, September 24, 2019. https://www.statista.com/statistics/610271/worldwide-personal-computers-installed-base/

[2] Statista, Number of smartphone users worldwide from 2016 to 2021 (in billions), as viewed, September 24, 2019. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[3] IOT Analytics, State of the IoT 2018: Number of IoT devices now at 7B—Market accelerating, August 8, 2018. https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

[4] Alana Semuels, Millions of Americans Have Lost Jobs in the Pandemic—And Robots and AI Are Replacing Them Faster Than Ever, Time, August 6, 2020. https://time.com/5876604/machines-jobs-coronavirus/

> In a recent Gartner CFO survey, **74% of companies** said they intend to shift employees to **work from home permanently**. The first company to implement this was Facebook, announcing it will permanently shift 50% of its employees to remote work.

FACT 1

This is permanent

Due to COVID-19, “click-economy” thinking is taking over in boardrooms. Part of the financial efficiency of companies like UBER and Airbnb comes from their use of affiliates’ assets rather than having to capitalize critical assets themselves. Likewise, freed by COVID-19 from policies that force employees to work at centralized offices, CFOs' are looking to realize immense cost savings from abandoning their commercial real estate by using employees' homes as places of business.[5] According to Kate Lister, president of Global Workplace Analytics, a typical employer can save about $11,000 per year for every employee who works remotely half of the time.[6] Considering the costs of heating and air conditioning, bandwidth, and other facilities costs as well as the burden of scaling real estate for growth and recessions, you can expect virtualizing employees and other stakeholders is here to stay.

When transitioning networking and cyber security, you should plan for the completely distributed computing environment to become permanent. Practically speaking, this means network and security professionals should avoid temporary stop-gap measures. It also means planning to accelerate cloud/ SaaS adoption for the following reasons.

[5] Jessica Davis, CFOs: COVID-19 Work-from-Home Plans May Be Permanent, InformationWeek, April 21, 2020 https://informationweek.com/strategic-cio/security-and-risk-strategy/cfos-COVID-19-work-from-home-plans-may-be-permanent/d/d-id/1337576

[6] Global Workplace Analytics, Work-at-Home After COVID-19—Our Forecast, https://globalworkplaceanalytics.com/work-at-home-after-COVID-19-our-forecast

FACT 2

Hello cloud, goodbye data centers

Providing connectivity to completely distributed users, IoT devices, branch offices and edge facilities will cause data bottlenecks if you backhaul all connections to a centralized data center. To avoid service latency, the new networking model calls for all applications to be cloud and SaaS hosted. This way, applications will transact data directly with nodes in the distributed environment without being held up at a central data center. Due to all-cloud /SaaS connectivity, cyber-security controls must also be native to the cloud, such as Firewall as a Service (FaaS). Security controls must also transition from centralized perimeter security to being purpose-built for securing cloud and SaaS workloads.

> “ No discussion on digital solutions should be held without considering cybersecurity. Any rapid adoption of emerging technologies will be a waste of time without securing the solutions you choose to employ.”[7]

FACT 3

Policies become paramount

As distributed access to cloud applications through VPNs and SD-WANs becomes the norm, it is important to focus more on policies. Networking policies are needed to prioritize traffic to protect service levels. For example, VoIP traffic can’t take much latency, but email is more tolerant to latency. Likewise in security, policies based on user identity will become more important to create Zero-trust networks to prevent attacks and limit damage inflicted by malicious insiders and outsiders armed with stolen credentials. In both networking and security, policies based on user identities pulled from directory services to control application access and prioritize traffic will grow in importance.

[7] Priya Merchant, 5 Digital Solutions to Help Your Business Take Off, Entrepreneur, October 13, 2020, https://www.entrepreneur.com/article/357079

> “ Ransomware’s economic model capitalizes on the misconception that a ransomware attack is solely a malware incident, whereas in reality ransomware is a breach involving human adversaries attacking a network.”[8]

FACT 4

Prevention is key

The COVID-19 pandemic’s reshaping of networks is causing a fair amount of pandemonium in IT and cyber security operations. Attackers are taking advantage of the confusion. Ransomware in particular is making a comeback[9] because organizations are transitioning to remote workforces. Under these circumstances, preventing malware and other types of attacks from entering the distributed environment is key to effective security. Advanced threat prevention that triggers threats within a virtual environment outside the production environment is critical to add to signature-based security and behavioral analysis. Simply detecting threats and remediating damage has become ineffective against today’s multivector and polymorphic threats and has become overly burdensome to security operations.

[8] Tom Burt, Microsoft Digital Defense Report, Microsoft, September 2020 https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/

[9] Danny Palmer, Ransomware: Surge in attacks as hackers take advantage of organisations under pressure, ZDNet.com, October 7, 2020. https://www.zdnet.com/article/ransomware-surge-in-attacks-as-hackers-take-advantage-of-organisations-under-pressure/?ftag=TRE-03-10aaa6b&bhid=29524966930760714833143964508637&mid=13095506&cid=2326675408

> “With every new attack or vulnerability, the red flags start to wave. The usual reaction is for organizations to review and consider ramping-up security with new products, with the assumption that these will help to better protect their networks and data. But will they? Or does adding more products from different vendors simply add more complexity, and potentially undermine security?”[10]

5 FACT

Consolidate security

Reworking your network strategy to meet the challenges of the pandemic changes where and how you provide security, but not the types of security you need:

- Cloud and SaaS application security
- Secure VPN, SD-WAN connectivity
- Endpoint protection for users
- Mobile device security
- Data protection: DLP/file encryption/ransomware file-backup
- Advanced antimalware/intrusion prevention/antivirus
- Zero-Trust access control

Redoing your security stack using point solutions means managing and monitoring up to 60 separate user interfaces. Under these conditions, on one hand, security breaches can be difficult to discover. On the other hand, a single multivector attack can trigger a security event storm.

In contrast, utilizing a consolidated security architecture with a single management interface for all security engines simplifies monitoring, administration, and management. This greatly reduces staff burden and costs. In addition, a unified security architecture supports the sharing of threat information among security engines, which further eliminates security gaps.

[10] Brian Gleeson, Cutting complexity to strengthen security: why consolidation matters, Check Point blog https://blog.checkpoint.com/2020/06/12/cutting-complexity-to-strengthen-security-why-consolidation-matters/

Conclusion

The COVID-19 pandemic has permanently changed the shape of IT and cyber security. Data centers are receding in importance, traffic and user access policies are gaining in prominence, and the case becomes even stronger for consolidated security that is preventative in nature and purpose-built to protect cloud/SaaS workloads. While this kind of forced change is challenging, it also opens the way for new opportunities to operate more efficiently throughout an organization.

For a perspective on what Check Point Software recommends to prepare you during the COVID-19 pandemic, click here.

To get information on Check Point Software and our cyber security solutions, visit our website.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com